### PATENT ABSTRACTS OF JAPAN

(11) Publication number:

11215122 A

(43) Date of publication of application: 06.08.99

(51) Int. CI

H04L 9/36

G09C 1/00

(21) Application number: 10013727

(71) Applicant:

MATSUSHITA ELECTRIC IND CO

LTD.

(22) Date of filing: 27.01.98

(72) Inventor:

HARADA TOSHIHARU OKUMURA YASUO

TATEBAYASHI MAKOTO

SAIJO TAKESHI ONO TAKATOSHI

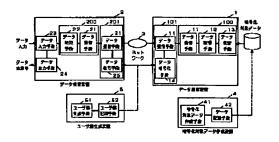
## (54) METHOD, DEVICE, AND SYSTEM FOR **ENCIPHERING DATA**

### (57) Abstract:

PROBLEM TO BE SOLVED: To provide a method, device, and system for enciphering data by which only the necessary scope of data distributed through WWW(world-wide web) can be enciphered in accordance with the contents of the data.

SOLUTION: (1) A data receiver 2 transmits data request information and receiver identification information when a user inputs data required by the user in a WWW browser 200. (2) A data transmitter 1 enciphers the data to be enciphered corresponding to the data requesting information and incorporating an enciphering scope designating instruction within the extent designated by the enciphering scope designating instruction in such a way that only the receiver can decode the enciphered data in an enciphering proxy 101 and transmits the results to the data receiver 2. (3) The data receiver 2 decodes the enciphered data in a decoding proxy 201 and outputs the decoded data.

COPYRIGHT: (C)1999,JPO



28

(11)特許出顧公園番号

(43)公開日 平成11年(1999)8月6日 特開平11-215122

G09C	H04L	(51) Int Q.
1/00	9/36	
660		<b>经</b> 別記号
G09C	H04L	۴I
1/00	9/00	
660Z	685	

存金組織 未超級 超级级の数15 〇L (全19月)

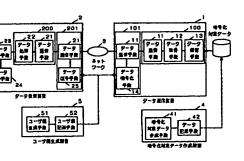
が共気に扱く	<b>10</b>				
į	,				
	(74) 代码 人中国十二省大学的少(人) 人(人)	(74) (P.M. )			
	<b>重操株式会社内</b>				
产	大阪府門其市大学門真1006番地 松下電器				
	<b>密学 夏</b>	(72) 発明者			
	<b><b> 连架株式会社内</b></b>				
常	大阪府門真市大学門真1006番地 松下電器				
	英村 康男	(72) 発明者			
	避業株式会社内				
穹	大阪府門其市大学門真1006番地 松下電器				
	原田 俊治	(72) 発明者			
	大阪府門其市大字門真1006番地		平成10年(1998) 1月27日	(22)出版日	•
	松下電器産業株式会社				
	000005821	(71)出版人 00005821	特置平10-13727	(21)出國番号	

(54) 【発明の名称】 データ暗号方法、データ暗号装置、及びデータ暗号システム

(57) 【聚念】

ステムを提供する。 に応じて必要な範囲だけを暗号化する方法、装置及びご 【課題】 WMYで配信されるデータに対して、その内容

る。(2)データ送信校の1は、時号プロキシ101にお けとると、データ要求情報と受信者識別情報を送信す 00において、ユーザから取得したいデータの入力を受 泉データを復号し、復号されたデータを出力する。 は、復身プロキシ201において暗号化された暗号化対 データ受信装置2に送信する。(3)データ受信装費2 れた受信者のみが復身できるように暗号化しこの結果を 指定命令で指定された範囲を、受信者識別指棋で指定さ が狙み込まれた啞号化対象データに対して、啞号化範囲 いて、データ要求格報に対応した、略号化続阻指定命令 【解決手段】 (1)データ受信装置 2 は、WMプラウザ



【特許請求の範囲】

を行なうデータ暗号方法であって、 組み込まれた命令に従って暗号化処理を含むデータ処理 定する命令が組み込まれた暗号化対象アータに対して、 【請求項1】暗号化処理方法を含むデータ処理方法を指

命令で指定された範囲を暗号化することを特徴とするテ **時号化する範囲を指定する時号化範囲指定命令が組み**込 一夕暗号方法。 まれた暗号化対象データに対して、前記暗号化範囲指定

定する受信者指定命令が狙み込まれている場合に、 指定命令に加えて、前記略号化対象データの受信者を指 【請求項2】前記暗号化対象データに、前記暗号化範囲

のデータ暗号方法。 を暗号化するようにしたことを特徴とする醇求項1記載 のうち、前記時号化誌囲指定命令により指定された範囲 題に対応する暗号化鍵を用いて、前記暗号化対象データ 前記受信者指定命令で指定された受信者が保持する很易

号化された前記第1の復号鍵を指定する鍵情報指定命令 信者の保持する第2の復号観に対応する第2の暗号化観 を組み込んだ暗号化データを得るようにしたことを特質 で暗号化し、暗号化された前記暗号化対象データに、明 し、前記等1の暗号化鍵に対応する第1の復号鍵を、曼 とする請求項1記載のデータ暗号方法。 【請求項3】前記略号化対象データを暗号化するに際 」、前記昭号化対象データを第1の暗号化銀で暗号化

データ暗号方法であって、 まれた命令に従って復号処理を含むデータ処理を行なう する命令が組み込まれた暗号化データに対して、組み込 【請求項4】彼号処理方法を含むデータ処理方法を指定

役号する範囲を指定する復号範囲指定命令が組み込まれ された範囲を復号することを特徴とするデータ暗号方 た暗号化データに対して、前記復号範囲指定命令で指定

定命令が狙み込まれている場合に、 令に加えて、暗号化データの受信者を指定する受信者指 【訪求項5】前記略号化データに、前記復号範囲指定命

号するようにしたことを特徴とする請求項4記載のデー 指定命令により指定された範囲を前記復号題を用いて復 前記受信者指定命令で指定された受信者が保持する復号 鍵を用いて、前記暗号化データに対して、前記復号範囲

健惰報指定命令が組み込まれている場合に、 令に加えて、暗号化された前記第1の復号観を指定する 【緯求項6】前記暗号化データに、前記復号範囲指定命

者の保持する第2の復号鍵で、復号し、 前記吗号化データを復号するに際し、前記聲惰報指定命 令で指定された暗号化された前記第1の復号鍵を、受信

鍵を用いて復号するようにしたことを特徴とする間求項 前記役号範囲指定命令により指定された範囲を前記復号 前記暗号化データを、復号された前記第1の復号級で、

4 記載のデータ暗号方法:

定用の命令を利用し、そのコメントとしてあらかじめ定 みなすようにしたことを特徴とする請求項1から6のう ための命令群の中から対応する命令が指定されたものと 記述方法として、前記HTMLで危殺されているコメント情 払びいた命令である場合に、原号処理のための命令群、 が、特に、HTML(Hypertext Warkup Language)質語に ちいずれか1項記載のデータ暗号方法。 めた特定のコメントが指定された時に前述の既号処理の 令、前記受信者指定命令、及び、前記題情報指定命令の すなわち前記暗号化範囲指定命令、前記復号範囲指定命 【請求項7】前記時号化対象データに組み込まれる命令

を行なうデータ時号数置であって、データ通信手段と、 組み込まれた命令に従って暗号化処理を含むデータ処理 定する命令が狙み込まれた暗号化対象データに対して、 データ取得手段と、データ保管手段と、データ暗号化手 【請求項8】暗号化処理方法を含むデータ処理方法を指

された範囲を暗号化し、この結果として得られる少なく 管手段から取得し、前記データ暗号化手段が、前記暗号 何報で要求された前記略号化対象データを前記データ保 受信したとき、前記データ取得手段が、前記データ要求 た邸号化対象データの送信を要求するデータ要求情報を 前記データ通信手段が、前記データ保管手段に保管され とするデータ暗号装置。 化データを作成し、データ通信手段が、前記暗号化デー する範囲を指定する彼号範囲指定命令を組み込んだ時号 とも一部が暗号化された前記暗号化対象データに、復号 化対象データのうち前記略号化模照指定命令により指定 タを前記データ要求情報の発信元に送信することを特別

昭号化手段を有する暗号化プログラムとが実装されたコ 段を備えたWYM(World Wide Web)サーバと、前記データ ンピュータであることを特徴とする結束項8記載のデー 通信手段と、前記データ取得手段と、前記データ保管手 夕晒号装置。 【蔚水項9】前記データ暗号装置が、特に、前記データ

を行うためのデータ通信手段を有するプログラムである 記略号化対象データもしくは前記略号化データの遊受信 号化手段に加えて、WMサーバまたはWMプラウザと、前 ことを特徴とする胡求項9記載のデータ略号装成。 【蔚東項10】前記暗号化プログラムが、前記データ暗

一タ復号手段を備え、 処理手段と、データ入力手段と、データ出力手段と、デ **うデータ暗号装置であって、データ通信手段と、デー**5 込まれた命令に従って很号処理を含むデータ処理を行な 定する命令が組み込まれた時号化データに対して、組み 【請求項11】復号処理方法を含むデータ処理方法を指

前記データ入力手段に、外部から取得したい暗号化対象 信手段が、前記時号化対象データの道信を要求するデー データを指定する情報が入力されたとき、前記データ通

時号化データのうち復身範囲指定命令で指定された範囲 復身する範囲を指定する復身範囲指定命令が組み込まれ 接続された前記データ出力手段に出力することを特徴と を復号し、前記データ処理手段が、復号された暗号化デ た時号化データを受信し、前記データ復号手段が、前記 するデータ暗号装低。 ータを、ディスプレやプリンタなどのデータ出力数囚が 夕要求情報を送信し、前記データ要求情報に対応する、

手段と、消配データ出力手段を備えたMMプラウザと、 のデータ時号数団。 前記データ復号手段を有する復号プログラムが災装され タ通信手段と、前記データ処理手段と、前記データ入力 たコンピュータであることを特徴とする蔚沢項11記載 【蔚求項12】前記データ受信装置が、特に、前記デー

手段に加えて、WWサーバまたはWWプラウザと、 【樹泉項13】前記復号プログラムが、前記データ復号

信を行うためのデータ通信手段を有するプログラムであ ることを特徴とする節求項12記載のデータ即号数四。 手段とを備えた送信側のデータ時号装置と、 データ保管手段と、データ暗号化手段と、ユーザ鹽保管 資配時号化対象データもしくは資配時号化データの送受 【荫沢玑14】データ通信手段と、データ取得手段と、

管手段とを備えた受信側のデータ暗号装置と、 と、データ出力手段と、データ復号手段と、ユーザ銀保 データ通信手段と、データ処理手段と、データ入力手段

ネットワークと、暗号化対象データ作成手段と暗号化な 象データ配送手段を備えた暗号化対象データ作成装取

保管し、前記很号號を前記受信側のデータ暗号装置のユ が、各ユーザ固有の暗号化量とこの暗号化量に対応する 生成数四とで構成されるデータ時号システムであって、 ーが観保管手段に保管し、 **鍵を前記送信側のデータ暗号装置のユーザ鍵保管手段に** 復号題を生成し、前記ユーザ酸配送手段が、前記時号化 育記ユーギ競生成数四において、預記ユーギ酸生成手段 ユーザ配生成手段とユーザ融配送手段を伺えたユーザ田

前記略号化対象データ作成装置において、前記略号化対 象データ作成手段が、暗号化する範囲を指定する暗号化 タを前記送信間のデータ暗号装置のデータ保管手段に保 前記時号化対象データ配送手段が、前記時号化対象デー 範囲指定命令を狙み込んだ暗号化対象データを作成し、

晒号化対象アータの送信を要求するアータ要求情報を前 手段に、外部から収得したい略号化対象データを指定す 前配受信調のデータ暗号装置において、前記データ入力 記送信側のデータ暗号装置に前記ネットワークを利用し る情報が入力されたとき、前記データ通信手段が、前記

前記送信側のデータ暗号装置において、前記データ通信 手段が、前記データ保管手段に保管された暗号化対象デ

> **号化し、この結果として得られる少なへとも一部が歴史** 前記データ取得手段が、前記データ要求情報で要求され のデータ略号装置に前記ネットワークを利用して送信 し、データ通信手段が、前記暗号化データを前記受信便 する復号範囲指定命令を組み込んだ暗号化データを作成 化された前記略号化対象データに、復号する範囲を指定 うち前記略号化範囲指定命令により指定された範囲を略 た前記啞号化対象データを前記データ保管手段から取得 ータの送信を要求するデータ要求情報を受信したとき、 し、前記データ暗号化手段が、前記暗号化対象データの

記データ処理手段が、復身された暗号化データを、ディ のうち復号範囲指定命令で指定された範囲を復号し、前 タを受信し、前記データ復号手段が、前記暗号化データ 記データ出力手段に出力することを特徴とするデータ暗 前記受信側のデータ暗号装置において、前記略号化デー スプレやプリンタなどのデータ出力装置が接続された前

管手段とを備えた受信側のデータ暗号装置と、ネットワ データ保管手段とを備えた送信側のデータ暗号装置と、 と、データ出力手段と、データ復号手段と、ユーザ段保 データ通信手段と、データ処理手段と、データ入力手段 【請求項15】データ通信手段と、データ取得手段と、

昭号化対象データ作成手段と、データ暗号化手段と、コ 化データ作成装置と、 ーザ競保管手段と、暗号化データ配送手段を備えた暗号

管し、前記復号鍵を前記受信仰のデータ暗号装匠のユー 鍵を前記略号化データ作成装置のユーザ観保管手段に保 が、各ユーザ固有の暗号化鍵とこの暗号化鍵に対応する 前記ユーザ酸生成装置において、前記ユーザ競生成手段 生成装置とで構成されるデータ暗号システムであって、 ユーザ錠生成手段とユーザ鍵配送手段を備えたユーザ鎖 ザ鍵保管手段に保管し、 復号離を生成し、前記ユーザ鍵配送手段が、前記暗号化

作成手段が、暗号化する範囲を指定する暗号化範囲指定 化データ配送手段が、前記町号化データを前記送信領の 指定命令を組み込んだ四号化データを作成し、前記屈号 暗号化対象データに、復号する範囲を指定する復号範囲 **枯果として仰られる少なくとも一部が唇母化された質質** 化範囲指定命令により指定された範囲を暗号化し、この 夕暗号化手段が、前記暗号化対象データのうち前記暗号 命令を担み込んだ昭号化対象データを作成し、前記デー 前記略号化データ作成装置において、前記略号化データ データ暗号装団のデータ保管手段に保管し、

信伽のデータ暗号装置に前記ネットワークを利用して送 暗号化データの送信を要求するデータ要求情報を前記送 手段に、外部から取得したい暗号化対象データを指定す 前記受信側のデータ暗号装置において、前記データ入力 る情報が入力されたとき、前記データ通信手段が、前記

> 暗号装置に前記ネットワークを利用して送信し、 タ通信手段が、前記暗号化データを前記受信側のデータ 記応号化データを前記データ保管手段から取得し、デー データ取得手段が、前記データ要求情報で要求された前 の送信を要求するデータ要求情報を受信したとき、前記 手段が、前記データ保管手段に保管された暗号化データ 前記送信側のデータ暗号装置において、前記データ通信

号システム。 記データ出力手段に出力することを特徴とするデータ暗 スプレやプリンタなどのデータ出力装置が接続された前 記データ処理手段が、復号された暗号化データを、ディ のうち彼母徳囲指定命令で指定された範囲を復号し、前 タを受信し、前記データ復号手段が、前記暗号化データ 前記受信回のデータ暗号装置において、前記暗号化デー

## 【発明の詳細な説明】

[1000]

伍、及びシステムに関する。 込まれた命令に従って昭号処理を施すための方法、装 理命令の組み込まれた暗号化対象データに対して、組み 【発明の属する技術分野】略号処理命令を含むデータ処

テムを探技する際のプラットフォームとして利用されつ 供するため急速に普及している。このため、WYDシステ った機能を、非常に簡便なユーザインターフェースで扱 チメディア情報の検索や、不特定多数への情報発信とい **ムを、パソコンソフトのオンライン販売など、商用シス** 【従来の技術】WWW(World Wide Web)システムは、マル [0002]

いようにするために、WMアータを暗号化することが考 分だけを暗号化するといった、きめ細かく暗号化するこ と称する)を、特定の受信者以外に盗聴(露見)される 電子情報や、部外後の電子情報(以下、単に9997データ えられる。また、特に商用利用の場合は、WMデータ とが考えられる。 を、その内容に応じて、一郎を規範可能とし、舡契な問 【0003】WWシステムを利用して発信される有料の

96年6月号(第7年)を参照されたい。 暗号化する方法としては、NetscapeCommunications社が らを用いるとMMデータは略号化されるため第三者への gration Technologies社が提唱するS-HTTPがあり、これ 提唱するSSL(Secure Socket Layer)や Enterprise Inte 盗聴(窈見)を防止することができる。なお、SSL及びS -HTTPについては、例えば、Q出版社のOPEN DESIGN、19 【0004】従来、WWシステムで発信する電子情報を

WMアータ全体に対して一律的に暗号化するものであっ の従来方法は、いずれも、BMTデータを発信するBMTサー バと、ロクイサデータを受信するロアカアプラウザ間で伝送される 【発明が解決しようとする課題】しかしながら、これら

が当由されたWWWサーバは、SSLに指力へ尽や政策が当知 号機能が追加された専用のWWサーバ及UMW/フラウザが ての受信者に視聴を可能とし、血要な部分だけを明号化 た。このため、WMアータの内容に応じて、一部はすべ されたWMプラウザとの間でのみ、WMデータの暗号通信 必敗であった。そして、例えば、SSLに指びへ略号仮信 た、従来方法では、上述のSSLまたはS-HTTPに基グへ略 するといった、きめ細かな啞号化が行えなかった。ま

を暗号化することも可能とする、データの暗号方法、製 データを暗号化するに際し、データの内容に応じて、必要な範囲だけを暗号化でき、また、必要であればあらか ステムを提供することを原2の目的とする。 号機能を追加する必要のない、すなわち、本発明のデー 低及びシステムを提供することを第1の目的とする。 方法、復号方法、暗号通信方法、及び、その装置及びシ サーバやWMTプラウザを必要としない、データの時号化 じめ指定した受信者のみが復号できるようにITMデータ タ母中代方法に指力へ母子教徒が当ちされた母用のIRM 【0006】本発明は、上記従来の問題点に鑑み、MM 【0007】また、既存のWMサーバやWMブラウザに暗

て、組み込まれた命令に従って暗号化処理を含むデータ 指定する命令が組み込まれた暗号化対象データに対し に、本発明は、暗号化処理方法を含むデータ処理方法を た範囲を暗号化する手段を備える。 泉データに対して、前記時号化範囲指定命令で指定され を指定する暗号化範囲指定命令が組み込まれた暗号化対 処理を行なうデータ暗号方法であって、暗号化する範囲 【課題を解決するための手段】上記目的を達成するため

者を指定する受信者指定命令が組み込まれている場合 復号銀に対応する暗号化盤を用いて、前起暗号化対象デ に、前記受信者指定命令で指定された受信者が保持する 化範囲指定命令に加えて、前記略号化対象データの受信 範囲を略号化する手段を備える。 ータのうち、何賀原号化徳照指院命令により指定された 【0009】また、前記暗号化対象データに、前記暗号

令を組み込んだ時号化データを得る手段を備える。 暗号化された前記券1の復号観を指定する観情報指定の 受債者の保持する第2の復号壁に対応する第2の暗号化 壁で暗号化し、暗号化された前記暗号化対象データに、 化し、前記祭1の暗号化鍵に対応する祭1の復号鍵を、 に際し、前記局号化対象データを第1の用号化器で码号 【0010】また、前記暗号化対象データを暗号化する

て、前記很号範囲指定命令で指定された範囲を復身する る復号範囲指定命令が組み込まれた暗号化データに対し 行なうデータ暗号方法であって、復号する範囲を指定す 組み込まれた命令に従って復号処理を含むデータ処理を を指定する命令が組み込まれた暗号化データに対して、 【0011】また、復号処理方法を含むデータ処理方法

手段を悩える。

指定命令に加えて、略号化データの受信者を指定する受 | 前院局号化データに対して、前記徴号範囲指定命令によ 定命令で指定された受信者が保持する很号段を用いて、 借者指定命令が組み込まれている場合に、前記受信者指 り指定された範囲を前配復号題を用いて復号する手段を 【0012】また、前記暗号化データに、前記役号範囲

時号化データを復身するに際し、前記鍵情報指定命令で 定する観情報指定命令が狙み込まれている場合に、前記 指定命令に加えて、暗号化された前記第1の復号壁を指 保持する第2の復号題で、復号し、前記暗号化データ 指定された暗号化された前記第1の復号題を、受信者の 【0013】また、前記町号化データに、前記復号範囲

命令により指定された範囲を前記復号鍵を用いて復号す を、復号された前記第1の復号観で、前記復号範囲指定 る手段を備える。

のとみなすようにする。 題のための命令群の中から対応する命令が指定されたも め始めた特定のロメントが指定された時に前述の即分類 党命令、前記受信者指定命令、及び、前記雖情報指定命 群、すなわち前記略号化範囲指定命令、前記復号範囲指 語に指力いた命令である場合に、時号処理のための命令 る命令が、特に、HTML(Hypertext Markup Language) 哲 今の記述方法として、前記HTMLで完成されているコメン ト指定用の命令を利用し、そのコメントとしてあらかじ 【0014】また、前記町号化対象データに組み込まれ

法を指定する命令が狙み込まれた暗号化対象データに対 管手段に保管された暗号化対象データの送信を要求する 号化手段を備え、前記データ通信手段が、前記データ保 段と、データ取得手段と、データ保管手段と、データ原 データ要求情報を受償したとき、前記データ取得手段 タ処理を行なうデータ時号装置であって、データ通信手 して、組み込まれた命令に従って暗号化処理を含むデー 【0015】また、暗号化処理方法を含むデータ処理方

が、前記データ要求惰報で要求された前記略号化対象デ 対象データに、後号する範囲を指定する彼号範囲指定命 化手段が、前記略号化対象データのうち前記略号化範囲 ―タを前記データ保管手段から取得し、前記データ暗号 が、前記昭号化データを前記データ要求情報の発信元に 令を狙み込んだ暗号化データを作成し、データ通信手段 して母られる少なくとも一部が母号化された何哲母号化 指定命令により指定された英囲を野号化し、この結果と

データ通信手段と、前記データ取得手段と、前記データ れたコンピュータである。 データ暗号化手段を有する暗号化プログラムとが実装さ 保管手段を備えたWMV(World Wide Web)サーバと、前記 【0016】また、前記データ暗号装置が、特に、前記

【0017】また、前記略号化プログラムが、前記デー

送受信を行うためのデータ通信手段を有するプログラム と、前記暗号化対象データもしくは前記暗号化データの 夕哈号化手段に加えて、WMサーバまたはWMプラウザ

囲指定命令で指定された範囲を復号し、前記データ処理 号範囲指定命令が組み込まれた暗号化データを受信し、 力されたとき、前記データ通信手段が、前記暗号化対象 行なうデータ暗号装置であって、データ通信手段と、デ 組み込まれた命令に従って復号処理を含むデータ処理を を指定する命令が組み込まれた暗号化データに対して、 手段が、復号された暗号化データを、ディスプレやプリ 前記データ復号手段が、前記暗号化データのうち復号範 データ要求情報に対応する、彼号する範囲を指定する彼 データの送信を要求するデータ要求情報を送信し、前記 部から取得したい暗号化対象データを指定する情報が入 と、データ復号手段を備え、前記データ入力手段に、外 ータ処理手段と、データ入力手段と、データ出力手段 ンタなどのデータ出力装置が接続された前記データ出力 【0018】また、復号処理方法を含むデータ処理方法

データ通信手段と、前記データ処理手段と、前記データ **がれたコンアュータたある。** と、前記データ復号手段を有する復号プログラムが実装 入力手段と、前記データ出力手段を備えたWMTブラウザ 【0019】また、前記データ受信装置が、特に、前記

記略号化対象データもしくは前記略号化データの送受価 復号手段に加えて、WMサーバまたはWMプラウザと、前 を行うためのデータ通信手段を有するプログラムであ 【0020】また、前記復号プログラムが、前記データ

歴生成装置において、前記ユーザ歴生成手段が、各ユー を指定する暗号化範囲指定命令を組み込んだ暗号化対象 て、前記時号化対象データ作成手段が、暗号化する範囲 信仰のデータ暗号装置のユーザ盤保管手段に保管し、前 成し、前記ユーザ館配送手段が、前配暗号化銀を前記送 ザ固有の暗号化鍵とこの暗号化鍵に対応する彼号鍵を生 で構成されるデータ暗号システムであって、前記ユーサ 成手段とユーザ鍵配送手段を備えたユーザ鍵生成装置と 手段を備えた暗号化対象データ作成装置と、ユーザ鍵生 と、暗号化対象データ作成手段と暗号化対象データ配送 とを備えた受信側のデータ暗号装置と、ネットワーク ータ出力手段と、データ復号手段と、ユーザ鍵保管手段 通信手段と、データ処理手段と、データ入力手段と、デ 保管手段とを備えた送信側のデータ暗号装置と、データ 記略号化対象データを前記送信頼のデータ暗号装置のデ 手段に保管し、前記略号化対象データ作成装置におい 記復号鍵を前記受信側のデータ時号装置のユーザ鍵保管 データを作成し、前記昭号化対象データ配送手段が、前 【0021】また、データ通信手段と、データ取得手段 データ保管手段と、データ応号化手段と、ユーザ錠

> などのデータ出力装置が接続された前記データ出力手段 定命令で指定された範囲を復号し、前記データ処理手段 るデータ要求情報を受信したとき、前記データ取得手段 おいて、前記データ入力手段に、外部から取得したい暗 ータ保管手段に保管し、前記受信館のデータ暗号装置に が、彼号された暗号化データを、ディスプレやプリンタ データ復号手段が、前記暗号化データのうち復号範囲指 9 暗号装置において、前起暗号化データを受信し、前記 前記ネットワークを利用して送信し、前記受信側のデー が、前記時号化データを前記受信側のデータ暗号装置に 令を組み込んだ暗号化データを作成し、データ通信手段 対象データに、彼号する範囲を指定する彼号範囲指定命 して得られる少なくとも一部が暗号化された前記暗号化 指定命令により指定された範囲を暗号化し、この結果と 化手段が、前記暗号化対象データのうち前記暗号化範囲 ータを前記データ保管手段から取得し、前記データ暗号 が、前記データ要求情報で要求された前記暗号化対象デ 保管手段に保管された暗号化対象データの送信を要求す 略号装置において、前記データ通信手段が、前記データ 記ネットワークを利用して送信し、前記送信側のデータ するデータ要求情報を前記送信頼のデータ暗号装置に前 データ通信手段が、前記暗号化対象データの送信を要求 号化対象データを指定する情報が入力されたとき、前記

時号化範囲指定命令により指定された範囲を暗号化し、 位において、前記ユーザ鍵生成手段が、各ユーザ固有の ユーザ銀配送手段を備えたユーザ鍵生成装置とで構成さ **迎保管手段とを備えた受信側のデータ暗号装置と、ネッ** 手段と、データ出力手段と、データ復号手段と、ユーザ 暗号化データ配送手段が、前記暗号化データを前記送信 指定命令を組み込んだ暗号化対象データを作成し、前記 前記受信間のデータ時号装置のユーザ健保管手段に保管 記ユーザ麹配送手段が、前記暗号化麹を前記暗号化デー れるデータ時号システムであって、前記ユーザ健生成数 化手段と、ユーザ鍵保管手段と、暗号化データ配送手段 と、データ保管手段とを増えた送信側のデータ暗号装置 側のデータ暗号装置のデータ保管手段に保管し、前記受 範囲指定命令を組み込んだ暗号化データを作成し、前記 前記啞号化対象データに、復号する範囲を指定する復号 データ暗号化手段が、前記暗号化対象データのうち前記 し、前記時号化データ作成装置において、前記時号化デ タ作成装置のユーザ酸保管手段に保管し、前記復号鍵を 暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前 を備えた暇号化データ作成装置と、ユーザ鍵生成手段と トワークと、暗号化対象データ作成手段と、データ暗号 この結果として得られる少なくとも一部が暗号化された ータ作成手段が、暗号化する範囲を指定する暗号化範囲 【0022】また、データ通信手段と、データ取得手段 、データ通信手段と、データ処理手段と、データ入力

> のデータ時号装置に前記ネットワークを利用して送信 化データの送信を要求するデータ要求情報を前記送信仰 類が入力されたとき、前記データ通信手段が、前記暗引 に、外部から取得したい暗号化対象データを指定する情 記受信側のデータ時号装置において、前記時号化データ 前記データ取得手段が、前記データ要求情報で要求され ータの送償を要求するデータ要求情報を受償したとき、 通信手段が、前記データ保管手段に保管された暗号化デ データ出力手段に出力する。 データ処理手段が、復号された暗号化データを、ディス うち彼号範囲指定命令で指定された範囲を復号し、前記 を受信し、前記データ初号手段が、前記暗号化データの データ通信手段が、前記暗号化データを前記受信期のデ た前記時号化データを前記データ保管手段から収得し、 し、前記送信側のデータ暗号装置において、前記データ **プレやプリンタなどのデータ出力製匠が模様された前盤** ―夕晴号装置に前記ネットワークを利用して送信し、前

text Markup Language)目指に指づいて、各種データ処 バを利用し、また、データを受信するデータ受信装匠と は、データを送信するデータ送信装匠として、MMサー いて、図面を用いて説明する。なお、本収描の形態で 理命令が組み込まれる場合について説明する。 配信されるデータの標準的な記述哲語であるHTML (Hyper 【0024】また、送信されるデータは、WMサーバで して、WMTプラウザを利用する場合について説明する。 【発明の攻摘の形態】以下に、本発明の災熵の形態につ

式およURSA暗号方式については、例えば関本英司客、 昭号方式を利用する場合について説明する。DES町号方 夕蝕と称する)の暗号化には、RSA暗号方式等の公開館 cryption Standard) 略号方式等の共通鏡暗号方式を利 用し、データの暗号化に利用した暗号化鍵(以下、デー 「暗号理論入門」共立出版(第3章及び第5章)を参照 【0 0 2 5】また、データの時号化には、DES (Data En

のデータ)を格納しておき、データ送信装位にて、デー 泉データを暗号化し、得られた暗号化データをデータ受 **夕受信装置からの送信要求に対応して、該当の暗号化対** あらかじめ暗号化対象データ(暗号化されていない平文 データを復号して取得する場合について説明する。 信裝仮に送信し、データ受信製度にて、受信した時号化 【0026】(現施の形態1)まず、データ送信装面に

ある。図1に示すようにデータ時号通信システムは、デ システム構成の既略について説明する。図1は、本災施 そして、本システムの動作辞細について説明する。 ータ送信装位1と、データ受信装位2と、これらを接続 の影談におけるデータ暦号追信システムの質易儀及囚ぐ に、本システムで扱うデータの構造について説明する。 【0028】「システムの擀成」本実施の形態の全体の

【0027】まず、システム構成について説明し、坎

信餌のデータ暗号装置において、前記データ入力手段

するネットワーク3と、暗号化対象データ作成装置4 と、ユーザ健生成装置5によって構成される。

いる。データ暗号化手段には、図示していないがユーザ WWWサーバの備えるデータ通信手段11が、WWWサーバと やワークステーションなど) が利用できる。この場合、 ationサーバなど)を実扱したコンピュータ(パンコン 鍵を保管するための公開鍵保管手段を備えている。デー データを生成するためのデータ暗号化手段14を備えて 指定命令にて指定された受信者向けに暗号化して暗号化 対象データを受信者識別情報もしくは後で述べる受信者 成される暗号化データを取得し、この暗号化データをデ WW/プラウギ図の超製過館プロトコルであるHTTPプロト 化対象データを保管するデータ保管手段13と、暗号化 ータ通信手段に渡すためのデータ収得手段12と、暗号 ータをデータ暗号化手段14に渡し、その結果として生 をデータ保管手段13から取り出し、この暗号化対象デ 報を受信しそのデータ要求情報に対応した暗号化データ らのデータ要求情報及びオプションとして受信者識別常 ロルに枯んいてアータ追信を行う。 えば、Netscape Communications社のNetscape Communic 手段を備えた、既存のWMM(Norld Wide Web)サーバ (例 上記データ通信手段と、データ取得手段と、データ保管 魔生成数位 5 によって生成された各ユーザのユーザ公団 1 と、上記データ要求情報に対応する暗号化対象データ 夕町号化手段14の胖相例以については後で説明する。 をデータ受信装置2に送信するためのデータ通信手段! 【0029】データ送信装匠1は、データ受信装匠2カ 【0030】データ送信装匠1としては、具体的には、

すように、CGIプログラムを利用する場合は、データ送 teway Interface) プログラム (各種データ処理機能をN ムとして動作する。すなわち、CCIプログラムを利用す 信袋低は、データ暗号化手段を提供するCCIプログラム する場合の構成図を図2 (1) に示す。図2 (1) に示 14の実現方法としては、具体的には、CGI (Common Ga る場合、MMサーバ毎にCCIプログラムを追加する必要か プログラム101と\\\\+ーバ100は一体のプログラ 101が組み込まれたWWサーバ100で構成され、CG データ送信数欧1を、WWサーバとCCIプログラムで実現 【0031】データ送信装置におけるデータ暗号化手段

信製田の構成図を図2 (2)に示す。 ともできる。暗号化プロキシで実現する場合のデータ送 グラム (以下、啞号化プロキシと称する) を利用するこ 化手段14の別の実現方法として、暗号化処理代行プロ 【0032】なお、データ送信装置におけるデータ暗号

パと暗号化プロキシで構成した場合のシステムの全体構 【0033】また、図3に、データ送信袋囚をWMサー

【0034】図2 (2) 及び図3に示すように、暗号化

ータ通信手段15を備えた暗号化プロキシ102で構成 プロキシによる構成を利用する場合は、データ送信装置 1は、〒Mサーバ100と、データ暗号化手段14とデ

通信のための標準プロトコルであるHTTPプロトコルに益 夕通信手段15は、WWWサーバとWWWブラウザ間のデータ **少いてデータ通信を行う。** 【0035】 ここで暗号化プロキシ102におけるデー

ができ、また、複数のMMサーバに一つの暗号化プロキ 動作させることが可能となる。そして、その結果、TMT シでデータ暗号化手段を追加することも可能となる。 サーバとして既存のWWサーバをそのまま利用すること 化プロキシ102は、それぞれ独立のプログラムとして 【0036】この構成により、MMサーバ100と暗号

得られる復号された暗号化データに対して、各種データ 暗号化データをデータ復号手段に渡し、その結果として ータを受信するためのデータ通信手段21と、受信した 置 1 にデータ要求惰報及びオプションとして受信者識別 にデータを出力するためのデータ出力手段24を備えて 印刷などのためにディスプレやプリンタなどの外部装備 ためのデータ入力手段23と、データの表示やデータの の保存やデータの印刷などの処理の指定など)を受ける するためのデータ復号手段23と、ユーザから各種デー 号化データを復号して、復号された暗号化データを生成 劇などの処理)を施すためのデータ処理手段22と、暗 処理(例えばデータの表示、データの保存、データの印 情報を送信し、そのデータ要求情報に対応した暗号化デ タ処理の指定(例えば取得したいデータの指定、データ 【0037】また、データ受信装置2は、データ送信装

生成装置 5 によって生成されたユーザ秘密器(このデー 25の詳細構成については後で説明する。 るための公開鍵保管手段を備えている。 データ復号手段 夕受信装匠を利用するユーザのユーザ秘密鍵) を保管す 【0038】データ復号手段には、図示していないが鎖

備えるデータ通信手段21が、WMサーバとWMプラウサ r) を実装したコンピュータ (パソコンやワークステー tscape Navigatorや、Microsoft社のInternet Explore **勢が接続されている。** できる。またデータ出力手段にはディスプレやプリンタ てデータ通信を行う。また、データ入力手段としては、 国の森母追儺プロトロックもるHTPプロトロッに指力で ションなど)が利用できる。この場合、WWアラウザの のWWTプラウザ(例えば、Netscape Communications社Ne 上記データ通信手段と、データ処処理手段を備えた既存 上記コンピュータの備えるキーボードやマウス枠を利用 【0039】データ受信装置2としては、具体的には、

プラグイン (各徴データ処理機能をRVN/プラウザに追加 25の実現手段としては、具体的には、MMプラウザの 【0040】データ受信装置2におけるデータ彼号手段

> 手段の構成図を図2 (3) に示す。図2 (3) に示す』 は、データ復号手段を提供する復号プラグイン201が タ復号手段を、プラグインで実現する場合のデータ復号 するためのプログラム)を利用することができる。デー **ザと復号プラグインは一体のプログラムとして動作す** 組み込まれたWMアラウザ200で構成され、WMアラウ うに、プラグインを利用する場合は、データ受信装置

Wブラウザ毎にプラグインを追加する必要がある。

手段14の別の実現方法として、復号処理代行プログラ 装置をMMプラウザと復号プロキシで構成した場合のシ きる。復号プロキシで実現する場合のデータ受信数置の 構成図を図2(4)に示す。また、図3に、データ受信 ム(以下、復号プロキシと称する)を利用することもで 【0042】なお、データ受信装置におけるデータ復号

ロキシによる構成を採用する場合は、データ受信教団 2 てデータ通信手段21を備えた復号プロキシ202で構 は、MMプラウザ200と、データ復号手段23に加え [0043] 図2 (4) 及び図3に示すように、復身プ

データ通信を行う。 ための標準プロトロルであるHTPプロトコルに描少いた 通信手段は、IMTサーバとIMTプラウザ間のデータ通信の 【0044】ここで彼号プロキシ202におけるデータ

号プロキシ202は、それぞれ独立のプログラムとして データ復号手段を追加することも可能となる。 ブラウザとして既存のRMTプラウザがそのまま利用で

号化対象データを作成する暗号化対象データ作成手段も データ保管手段13に配送するデータ配送手段42が備 【0046】暗号化対象データ作成装置4としては、暗 1と、作成した暗号化対象データをデータ送信装置1の

的には、通常のテキストエディターや既存のWMデータ ンで配送する手段等をとることができる。

信装置の秘密銀保管手段に配送するとともに、生成した は、後で説明する。ユーザ鍵生成装置5は、各ユーザ毎 に固有のユーザ秘密鍵及びユーザ公開鍵を生成するユー ザ頭生成手段51と、生成したユーザ秘密題をデータ受 【0048】暗号化対象データのデータ構造について

【0041】すなわち、プラグインを利用する場合、暗

ステムの全体構成を示す。

き、また、複数のMMアラウザに一つの復号プロキシで 動作させることが可能となる。そして、その結果、WM 【0045】この緯成により、YMTアラウザ200と復

ーション)が利用できる。またデータ配送手段42の具 エアが実装されたコンピュータ (パソコンやワークステ 体的な実現方法としては、例えば、暗号化対象データを フロッピーディスクなどの記録媒体に記録してオフライ (ホームページなど)を作成するための市販のソフトウ 【0047】暗号化対象データ作成装置4として、具体

ユーザ公開鍵を、データ暗号化装置の公開健保管手段に 的に安全な媒体に記録してオフラインで配送する手段 ーザ鍵配送手段としては、例えば、ICカードなどの物理 とが利用できる。またユーザ秘密観を配送するためのユ プログラムを実装したパソコンやワークステーションな 配送するためのユーザ酸配送手段52を備えている。ユ ―ザ陸生成装置5としては、具体的には、ユーザ最生成

と証明音をキットワークを利用してオンタインで冗子的 証明書を、フロッピーディスクなどの記録媒体に記録し 送する手段や、認証局と呼ばれる公的機関にユーザ公開 公開鍵を配送するためのユーザ鍵配送手段としては、例 送する手段などを利用することができる。また、ユーザ 暗号化されたユーザ協密鍵をネットワークを利用して配 の記録媒体に記録して配送する手段や、パスワード等で 健略号方式により略号化した上でフロッピーディスク等 や、ユーザ協密鍵をユーザのパスワード等を用いて共通 てオフラインで配送する手段や、または、ユーザ公開級 鍵に対する証明的の発行を受けた上で、ユーザ公開鍵と えば、1Cカードなどの物理的に安全な媒体に起録して配 に配送する手段などを利用することができる。

成も可能である。 について説明したが、これらの製匠を同じコンピュータ 生成校匠5は、それぞれ異なる技匠として実現する場合 夕受信装置と、ユーザ鎧生成装置の各機能を持たせる構 るコンピュータに、暗号化対象データ作成装置と、デー で実現することも可能である。例えば、ユーザの利用す タ受信穀匠2、暗号化対象データ作成装匠4、ユーザ題 【0049】なお、ここでは、データ送信装<u></u> 1、デー

として得られる暗号化データのデータ構造について説明 対象データを組み込まれた命令に従って暗号化した結果 処理命令が組み込まれた暗号化対象データと、この暗号 遺」次に、本実施の形態で扱う、晴号処理を含むデータ 【0050】「暗号対象データ及び暗号化データの構

いて作成する場合について説明するが、他の記述智語に 略号化データとして、WMデータの概率的な記述目語で 堪力いて同様に作成することも可能である。 ある、HTML(Hypertext Markup Language)質語に抜り 【0051】なお、ここでは、暗号化対象データおよび

時号化対象データD1は、通信のHTM、目指で記述された 者を指定する受信者指定命令C2などの暗号処理命令序が 号化範囲指定命令(1や、この暗号化対象データの受信 データ本体DOに、暗号化するデータ範囲を指定する暗 対象データの構造例である。図5 (1) に示すように、 追加された構造をとる。 【0052】図5(1)は、本実施の形照で扱う時号化

に、暗号化データD2は、復号する範囲を指定する復号 暗号化データの構造例である。図5(2)に示すよう 範囲指定命令(3や、この母号化データの交換者が復身す 【0053】また、図5(2)は、本実施の形態で扱う

-7-

C4などの時号処理命令時が迫加された構造をとる。 る際に利用する壁物類を指定するための壁物類指定命令

指定命令により、データ提供者は、提供するデータに対 することが可能となる。 して、必要に応じて、必要な範囲だけを略号化して扱り うち昭号化する徳田を指定する命令である。母母化徳田 おいて必ず指定される命令であり、略号化対象データの において、時号化徳囲指定命令は、時号化対象データに に組み込まれる時号処理命令罪の既について示す。 図 6 【0054】図6に、暗号対象データ及び暗号化データ

|正しく彼号できるように暗号化対象データを鳴号化す は、この受信者指定命令により指定された受信者のみか る。データの暗号化の群相構成については後で説明す 者をあらかじめ指定する命令である。受信者指定命令が 指定された場合、データ暗号化数四のデータ暗号化手段 定される命令であり、暗号化対象データを受信する受信 【0055】また、受信告指定命令は、必要に応じて指

供するデータが、復号できないように刻仰することが可 ることにより、あらかじめ指定した受信者以外には、提 【0056】データ提供者は、受信者指定命令を利用す

命令とは異なり単なるコメントとして扱われる(以下、 囲まれたデータを暗号化することを指定する。なお、こ とにより、既存のWMYサーバやプラウザに影響を与える SECRET->で呼号代類国の国始と終了を指定し、これらで 化したり、指定した受信のみが復号できるように暗号化 ことなく、データを必要に応じて必要な範囲のみを暗号 朝り当てている。このようにコメント命令を利用するこ 命令は、コメントとして無視され、MMTプラウザや、MMT のMMTプラウザや、MMTサーバにおいて、時号代徳田指定 この命令をコメント命令と称する)。 したがって、既存 こで、肝児母語では、文字列"<!\*\*\*-->は、通常の は、次のような文字列<!--BEGIN SECRET->と、<!--END するための命令を暗号化対象データに組み込むことが可 利用し、それぞれ特定の文字列を所定の暗号処理命令に ように他の応号処理命令も、HTML哲語のコメント命令を サーバに影響を及ぼすことはない。同様に、図りに示す 【0057】また、暗号化範囲指定命令は、具体的に

**号手段25の辞組構成について説明する。** 啞号化手段14と、データ受信装置2におけるデータ復 群和協成」ここでは、データ送信装置 1 におけるデータ 【0058】「データ暗号化手段及びデータ祖号手段の

を用いて、共通健略号方式により暗号化対象データのう 1と、データ競生成手段141にて生成されたデータ観 であるデータ壁を生成するためのデータ鍵生成手段14 は、暗号化対象データを暗号化する際に利用する、乱数 図4に示す。図4に示すように、データ暗号化手段14 【0059】まず、データ町号化手段14の群期構成を

> 銀暗号化手段144と、暗号化された暗号化対象データ から、受信者指定命令、もしくは、データ受信装置から 哲手段143において保管されているユーザ公開鍵の中 管するユーザ公開健保管手段143と、ユーザ公開健保 通銀時号化手段142と、各ユーザのユーザ公開錠を保 ち殴引化範囲指定命令で指定された範囲を暗号化する共 暗号化データ生成手段145より構成される。 化されたデータ鍵を指定する壁情報指定命令を追加する に、復号する範囲を指定する復号範囲指定命令や、暗号 て、公開銀昭号方式により、データ銀を昭号化する公開 ザ公開館を取り出し、取り出されたユーザ公開鍵を用い 受信した受信者識別情報により指定された受信者のユー

【0060】 データ復号手段13の詳細構成を図4

同じ共通健暗号方式を用いて、暗号化データのうち復号 段254より構成される。 範囲指定命令で指定された範囲を復号する共通鍵復号手 鍵を用いて、データ暗号化手段において利用したものと て復号する公開銀復号手段253と、復号されたデータ 手段において利用したものと同じ公開健暗号方式を用い 密館を用いて、暗号化されたデータ鍵を、データ暗号化 秘密避保管手段 252において管理されているユーザ協 手段254に渡すための暗号化データ解析手段251 のうち彼号範囲指定命令で指定された範囲を共通観復号 データ鍵を公開鍵復号手段253に渡し、暗号化データ た暗号化されたデータ鍵を取り出し、この暗号化された 段25は、暗号化データから顕情報指定命令で指定され と、ユーザ秘密観を保管する秘密観保管手段252と、 (2) に示す。図4 (2) に示すように、データ復号手

こついて説明する。 【0061】「詳細な動作」次に、本実施の形態の動作

の役、個々の処理の詳細動作について説明する。 [0062]まず、全体の動作販路について説明し、そ

の全体の助作概略を示すフローチャートである。 のユーザが利用を開始するときに行うユーザ鍵生成処理 【0064】図7に示すように、本実施の形態は、新規

図7は、本実施の形態におけるデータ暗号通信システム

【0063】(1) 本実施の形態全体の動作版路

取得するときに行うデータ取得処理(ステップS30 処理(ステップS200)と、ユーザが、提供データを (ステップS100)と、データの提供者が提供データ (暗号化対象データ)を作成するときに行うデータ作成

るデータ受信装匠に、またユーザ公開鍵を、データ送信 を生成し、生成したユーザ秘密鍵をそのユーザの利用す ユーザ協密鍵と、ユーザ協密鍵に対応するユーザ公開鍵 健生成装匠を利用して行う。具体的には、各ユーザ用の ユーザ自身、もしくは、本システムの管理者が、ユーザ 装囮に配送するなどの処理を行う。 【0065】 ここでユーザ鍵生成処理(S100)は、

【0066】 データ作成処理(S200) は、データ提

対象データを、データ送信装置に配送するなどの処理な 体的には、暗号化対象データを作成し、作成した暗号化 供者が、啞号化対象データ作成發置を利用して行う。具

から、そのデータ要求情報に対応する暗号化された暗号 化データを復号し取得するなどの処理を行う。 化対象データ (暗号化データ) を受信し、受信した暗号 タ要求情報をデータ送信装置に送信し、データ送信装置 提供データ(暗号化対象データ)の送信を要求するデー ーザが、自分のデータ受信装置を利用して、取得したい が、データ受信装置を利用して行う。具体的には、各ユ 【0067】 データ取得処理(S300)は、各ユーサ

【0068】(2) ユーザ鍵生成処理 (S100)の

図8は、ユーザ競生成処理の辞細動作を示すフローチャ

ユーザ鍵配送手段により、生成したユーザ秘密鍵を、第 り、各ユーザ用に、ユーザ秘密鍵とそのユーザ秘密鍵に テップS150)。 ザ公開發保管手段により、ユーザ公開鍵を保管する(ス ようにデータ送信装団のユーザ公開健保管手段に配送し り、生成したユーザ公開鍵を、第三者に改ざんされない し(ステップS130)、また、ユーザ銀配送手段によ いて、ユーザ秘密銀保管手段によりユーザ秘密盤を保管 段に配送し(ステップS120)、データ受信装置にお 三者に欲見しないようにデータ受信装匠の秘密健保管手 対応するユーザ公開題を生成し(ステップS110) は、ユーザ競生成装置において、ユーザ競生成手段によ (ステップS140)、データ送信装價において、ユー [0069] 図8に示すように、ユーザ競生成処理で

的な手段としては、ユーザ公開観に、公的な認証局の発 第三者により改ざんされないように配送するための具体 するなどの手段が利用できる。また、ユーザ公開鍵が 配送するか、または、ICカードを利用して手渡して配送 波しで配送するか、ネットワークを介してオンラインで 方式で略号化した後、フロッピーディスクに記録して手 配送するための具体的な手段としては、ユーザ秘密器 クやICカードに記録して手渡しで配送するなどの手段が 行した証明啓を添付して転送するか、フロッピーディス を、ユーザの指定したパスワードを用いて、共通銀暗号 【0070】ユーザ秘密鍵が第三者に露見しないように

【0071】 (3) データ作成処理 (S200) の群

図9は、データ作成処理の詳細動作を示すフローチャー

昭号化対象データ作成装置において、昭号化対象デーシ 作成手段により、暗号化範囲指定命令や受信者指定命令 などを組み込んだ暗号化対象データを作成し(ステップ [0072] 図9に示すように、データ作成処理では、

データを、データ送信袋匠のデータ保管手段に配送し 210)、データ配送手段により、作成した暗号化対象 銀データを保管する(ステップ220)。 (ステップ220)、データ送信装匠において、暗号化対

な実現方法としては、暗号化対象データをフロッピーな どの記録媒体に記録して手渡しで配送するなどの手段が 【0073】暗号化対象データを配送するための具体的

【0074】 (4) データ取得処理 (S300) の肆

まず、データ送信装団を、MMサーバとCGIプログラム は、この場合のデータ取得処理の群却動作を示すフロー で構成する場合の詳細動作について説明する。図13 で、データ受信装置を、NMTプラウザと復身プラグイン

若識別情報で指定された受信者のみが復分できるように 時号化対象データを、受信者指定命令、もしくは、受信 報をデータ送信装匠に送信し(ステップS320)、デ 定を受け取り(ステップS310)、データ通信手段に は、まず、データ受信装匠のMMプラウザにおいて、ユ し(ステップS370)、データ彼号手段により、吓号 信装置に送信し(ステップS360)、データ受信装置 報と、オプションとして受信者を指定する受信者煥別的 などのためにデータ出力手段に渡す (ステップS39 段により、復号された暗号化データを、ディスプレ表示 において、データ通信手段により、暗号化データを受信 昭号化して、昭号化データを作成し(ステップS35 ップS340)、データ暗号化手段により、取得された タ要求情報に対応する暗号化対象データを取得し(ステ ップS330)、データ取得手段により、受信したデー より、データ要求情報と受信者識別情報を受信し(ステ ータ送信装匠のWWサーバにおいて、データ通信手段に より、指定されたデータの送價を要求するデータ要求情 ーザ入力手段により、ユーザから取得したいデータの指 化データを複号し(ステップS380)、データ処理手 0)、データ通信手段により、暗号化データをデータ受 【0075】図10に示すように、データ取得処理で

命令の組み込まれたデータにおいて、その命令を実行す 接入力する方法や、取得したいデータのURLを指定する アドレス情報(データの保管場所を指定する情報)を直 orm Resource Location)と呼ばれる取得したいデータの ることによって行う方法などを利用できる。 が収得したいデータを指定する方法としては、URL(Unit 【0076】ここで、ステップS310においてユーザ

における暗号化対象データの暗号化 (ステップS35 【0077】また、図11 (1)は、データ暗号化手段

手段では、データ鍵生成手段により、データ観を生成し 0) の評価な動作を示すフローチャートである。 【0078】図11(1)に示すように、データ時身化

手段に保管されている各ユーザのユーザ公園館の中か 範囲指定命令で指定された範囲を時号化し(ステップS したデータ数を用いて、暗号化対象データのうち暗号化 公開鍵を利用して、公開鍵暗号化し (ステップS35 された受信者のユーザ公開館を取得し、取得したユーザ を組み込んだ町号化データを作成する(ステップ35 夕館を指定する時号館情報指定命令と復号範囲指定命令 3)、昭号化データ作成手段により、昭号化されたデー 6、外間者指信命令、もしへは、外間者は別情報で指定 352)、公開銀収号化手段により、ユーザ公開銀保管 (ステップS351)、共通短時身化手段により、生成

な助作を示すフローチャートである。 おける町号化データの復号(ステップS380)の辞載 【0079】また、図11(2)は、データ復号手段に

取得し (ステップ5381)、公開競役号手段により、 段では、暗号化データ解析手段により、暗号化データか 号された暗号化データを取得する (ステップS38 ら既情報指定命令で指定された暗号化されたデータ鍵を 用して暗号化データを復号し(ステップS383)、復 2)、共通政役号手段により、役号されたデータ競を利 ユーザ総密題保管手段に保管されたユーザ秘密題を用い て、町号化されたデータ鍵を復号し(ステップS38 【0080】図11(2)に示すように、データ復号手

信者識別情報を送信する必要はない。 を組み込むことにより、暗号化対象データの受信者を指 定する場合は、データ受信装置からデータ送信装置に受 【0081】なお、暗号化対象データに受信者指定命令

号化プロキシで、データ受信数囚を、MMプラウザと彼 示すフローチャートである。 る。図12は、この場合のデータ取得処理の詳細動作を **导プロキシで構成する場合の辞担動作について説明す** 【0082】次に、データ送信装匠を、WMサーバと時

は、まず、データ受債装置のWMVブラウザにおいて、ユ テップS440)、データ通信手段により暗号化対象デ 報を、データ送信装位に送信し (ステップS420)、 完を受け取り (ステップS410)、データ通信手段に ーザ入力手段により、ユーザから取得したいデータの指 化手段により、取得された暗号化対象データを、受信者 対象データを受信し(ステップS460)、データ環境 昭号化プロキシにおいて、データ通信手段により昭号化 ータを暗号化プロキシに送信し(ステップS450)、 一タ要求情報に対応する啞号化対象データを取得し(ス テップS430)、データ取得手段により、受信したデ により、データ要求情報と受信者類別情報を受信し(ス データ送信袋位のWMサーバにおいて、データ通信手段 報と、オプションとして受信者を指定する受信者識別情 より、指定されたデータの送信を要求するデータ要求情 【0083】図12に示すように、データ収得処理で

> S510)、〒Mプラウザのデータ通信手段により、復 スプレ表示などのためにデータ出力手段に渡す(ステッ 号された暗号データを受信し(ステップS520)、デ された暗号化データをWWプラウザに送信し(ステップ 90)、データ復身手段により、暗身化データを復身し 通信手段により、暗号化データを受信し(ステップS4 0)、データ受信装置の復号プロキシにおいて、データ 町号化データを復号プロキシに送信し(ステップS48 作成し(ステップS470)、データ通信手段により、 者のみが似号できるように略号化して、暗号化データを 指定命令、もしくは、受信者識別情報で指定された受信 ータ処理手段により、復身された暗号化データを、ディ (ステップS500)、テータ通信手段において、復号

信数置にて、受信した暗号化データを復号して取得する 当の暗号化データをデータ受信装置に送信し、データ受 位にて、データ受信装置からの送信要求に対応して、数 あらかじめ暗号化データを指納しておき、データ送信袋 場合について説明する。 【0084】(実施の形態2) 次に、データ送信装置に

に、本システムの辞細な動作について説明する。 【0085】まず、システムの構成について説明し、次

するネットワーク3と、暗号化データ作成装置6と、ユ る。図13に示すようにデータ暗号通信システムは、デ 憩におけるデータ暗号通信システムの概略構成図であ システム構成について説明する。図13は、本実施の形 ータ送信装置1と、データ受信装置2と、これらを接続 -ザ頭虫成装置5によって構成される。 【0086】「システムの構成」本実施の形態の全体の

生成教団の構成は、実施の形態1と同じものが利用でき るので、ここでは説明を省略する。 【0087】ここで、データ受信装置、及び、ユーザ限

報を受信しそのデータ要求情報に対応した暗号化データ 化データを保管するためのデータ保管手段13で構成さ ータ通信手段に渡すためのデータ取得手段12と、暗号 をデータ受信装置2に送信するためのデータ通信手段1 らのデータ要求情報及びオプションとして受信者識別情 - 夕保管手段13から取り出し、この暗号化データをデ 1 と、上記データ要求情報に対応する暗号化データをデ 【0088】データ送信装置1は、データ受信装置2か

MMプラウ井町の森母通信プロトコルであるHTTPプロト WMサーバの備えるデータ通信手段11が、WMサーバと やワークステーションなど) が利用できる。この場合、 ationサーバなど) を実装したコンピュータ (パソコン 手段を備えた、既存のWWW(World Wide Web)サーバ (例 上記データ通信手段と、データ取得手段と、データ保管 コルに協力いてデータ通信を行う。 えば、Netscape Communications社のNetscape Communic 【0089】データ送信装置1としては、具体的には、

> **格成については実施の形態1の場合と同じであるので数** 成された各ユーザのユーザ公開鍵を保管するための公開 化手段には、関示していないが鍵生成装置5によって生 号化データを生成するためのデータ暗号化手段62と、 信者指定命令にて指定された受信者向けに暗号化して暗 対象データを作成する暗号化対象データ作成手段61 避保管手段を備えている。データ暗号化手段14の詳細 配送するデータ配送手段63を備えている。データ暗号 暗号化データをデータ送信製置のデータ保管手段13に と、作成した暗号化対象データを暗号化対象データを受 【0090】暗号化データ作成装置6としては、暗号化

ン) が利用できる。 実装されたコンピュータ (パソコンやワークステーショ ア、及び、データ暗号化手段を実現するプログラムとが ームページなど)を作成するための市販のソフトウエ は、通常のテキストエディターや既存のRRNデータ(ホ 【0091】暗号化データ作成装置として、具体的に

手段等をとることができる。 イスクなどの記録媒体に記録してオフラインで配送する 法としては、例えば、暗号化対象データをフロッピーデ 【0092】またデータ配送手段42の具体的な実現方

タ供追については、実施の形態1の場合と同じであるの 【0093】暗号化対象データ及び暗号化データのデー

いついて説圧する。 [0094]「詳細な動作」次に、本実施の形態の動作

ユーザが利用を開始するときに行うユーザ鍵生成処理 動作既略としては、実施の影照1と同様であり、新規の 本実施の形団におけるデータ暗号通信システムの全体の の後、個々の処理の詳細動作について説明する。 [0095]まず、全体の動作既略について説明し、 【0096】(1) 本実施の形態全体の動作展局

を取得するときに行うデータ取得処理(ステップS30 成処理 (ステップS200) と、ユーザが、提供データ (暗号化データ)を作成するときに行う暗号化データ作

(ステップS100)と、データの提供者が提供データ

体的には、各ユーザ用のユーザ秘密観と、ユーザ秘密観 実施の形態1と同様に、ユーザ自身、もしくは、本シス テムの管理者が、ユーザ壁生成装置を利用して行う。具 ザ公開鍵を、データ送信装置に配送するなどの処理を行 鍵をそのユーザの利用するデータ受信装置に、またユー に対応するユーザ公開鍵を生成し、生成したユーザ秘密 【0097】 ここでユーザ競生成処理(S100)は、

隠1と具なり、データ提供者が、暗号化データ作成数国 [0098] データ作成処理 (S200) は、実施の形

【0099】具体的には、暗号化対象データを作成し

に配送するなどの処理を行う。 作成した暗号化対象データを暗号化し、データ送信装例

る暗号化データを受俗し、受信した暗号化データを復号 送信を要求するデータ要求价報をデータ送信装匠に送信 を利用して、取得したい扱供データ(暗号化データ)の 行う。具体的には、各ユーザが、自分のデータ受信袋医 隠1と異なり、各ユーザが、データ受信装置を利用して し、データ送信装匠から、そのデータ要求情報に対応す し取得するなどの処理を行う。 【0100】データ取得処理(S300)は、実施の影

【0101】(2) ユーザ競生成処理(S100)の

ユーザ鍵生成処理の動作は、疾歯の形態1の場合と同じ であるので説明は省略する。 [0102] (3) データ作成処理 (S200)の群

図14は、データ作成処理の群組動作を示すフローチャ

作成手段により、暗号化範囲指定命令や受信者指定命令 210)、暗号化対象データを、受信者指定命令で指定 は、暗号化データ作成数位において、暗号化対象データ 装配において、暗号化データを保管する(ステップ24 より、作成した暗号化対象データを、データ送信效性の 化データを作成し(ステップ220)、データ配送手段に された受信者のみが復身できるように時身化して、時号 などを担み込んだ時号化対象データを作成し(ステップ データ保管手段に配送し(ステップと30)、データ送伯 【0103】図14に示すように、データ作成処理で

形態 1 の場合と同様であるので説明は省略する。 タの暗号化(ステップS220)の緋細な動作は疾癌の 【0104】データ暗号化手段における暗号化対象デー

を利用してオンラインで配送するなどの手段が利用でき **媒体に記録して手渡しで配送する方法や、ネットワーク** 現力法としては、暗号化データをフロッピーなどの記録 【0105】暗号化データを配送するための具体的な実

【0106】(4) データ取得処理(S300)の牌

まず、データ受信装匠を、WMプラウザと征号プラグイ は、この場合のデータ取得処理の辞細動作を示すフロー ンで構成する場合の辞档動作について説明する。図15

より、指定されたデータの送價を要求するデータ要求情 は、まず、データ受信装匠のMMプラウザにおいて、ユ Wサーバにおいて、データ通信手段により、データ要求 定を受け取り (ステップS310) 、データ通信手段に ーザ入力手段により、ユーザから取得したいデータの指 報を送信し(ステップS320)、データ送信勢配のM 【0107】図15に示すように、データ取得処理で

にデータ出力手段に渡す (ステップS380)。 彼号された暗号化データを、ディスプレ安示などのため 復号し(ステップS370)、データ処理手段により、 プS360)、データ復号手段により、暗号化データを 信し(ステップS350)、データ受信装置において、 タ通信手段により、暗号化データをデータ受信装置に送 する時号化データを取得し(ステップS340)、デー データ取得手段により、受信したデータ要求情報に対応 情報と受信者雄別情報を受信し(ステップ5330)、 データ通信手段により、暗号化データを受信し(ステッ

場合と回復たあるのた説明は名略する。 号(ステップS370)の群相な動作は収施の形態1の 【0108】データ従号手段における時号化データの復

示すフローチャートである。 る。図16は、この場合のデータ取得処理の辞組動作を 復分プロキッス構成する場合の評価動作について説明す 【0 1 0 9】次に、データ受信装匠を、MMブラウザと

り、彼号された昭号化データを、ディスプレ表示などの 0)、データ通信手段において、復号された暗号化デー **号手段により、暗号化データを復号し(ステップS47** 暗号化データを受信し(ステップS460)、データ很 校四の役号プロキシにおいて、データ道信手段により、 号プロキシに送信し(ステップS450)、データ受作 ータ要求情報に対応する暗号化データを取得し(ステッ テップS430)、データ取得手段により、受信したデ により、データ要求情報と受信者識別情報を受信し(ス 報を、データ送信装位に送信し (ステップS420)、 完を受け取り (ステップS410)、アータ通信手段に は、まず、データ受信装匠のWMブラウザにおいて、ユ を受信し(ステップS490)、データ処理手段によ ラウザのデータ通信手段により、復身された暗号データ プS440)、データ通信手段により時号化データを復 データ送信装匠のWMサーバにおいて、データ通信手段 より、指定されたデータの送信を要求するデータ要求情 ためにデータ出力手段に渡す(ステップS500)。 タをIMMアラウザに送信し(ステップS480)、IMMフ ーザ入力手段により、ユーザから取得したいデータの指 【0110】図16に示すように、データ取得処理で

UMMを利用する場合について説明したがそれに限るも では、データの送信及びデータの受信に、mmサーバ及 【0112】また、データとして、HDA.宮語に茶づいて 【0111】なお、災極の形成1、及び、災極の形成2

いて規則したが、それに限るものではない。 各種データ処理の命令が組み込まれたデータの場合につ 場合について説明したが、それに限るものではない。 の時号化に共通銀磨号方式を利用し、データの暗号化に 利用したデータ鍵の略号化に公開鍵略号方式を利用する 【0113】また、テータの暗号化手段として、テータ

> むことにより、暗号化対象データは、暗号化範囲指定命 暗号化する範囲を指定する暗号化範囲指定命令を組み込 に応じて、暗号化対象データの重要な部分のみを暗号化 令で指定された範囲のみ暗号化される。このため、必要 したり、一部はすべての受信者に視聴させることが可能 【発明の効果】本発明によれば、暗号化対象アータに、

あらかじめ受信者を限定することが可能となる。 号化することが可能となる。すなわち、必要に応じて、 データを、指定した受信者以外は復身できないように暗 する受信者指定命令を組み込むことにより、暗号化対象 【0115】また、暗号化対象データに、受信者を指定

定された範囲のみを暗号化するためのデータ暗号化手段 号送信を行うデータ暗号装置が提供可能となる。 行うためのデータ通信手段とを備えた暗号化プログラム のNYMサーバを変更することなく利用した、データの暗 とを実装したコンピュータで绑成することにより、既存 とMMサーバ及びMMプラウザとの間でデータの送受信を バと、暗号化対象データのうち暗号化範囲指定命令で指 【0 1 1 6】また、特に、データ送信装置を、RMTサー

変更することなく利用した、暗号化データの復号受信を ラウザと、暗号化データのうち領号領囲指定命令な指院 行うデータ暗号装置が提供可能となる。 ピュータで構成することにより、既存のRMTプラウザを 通信手段とを備えた彼号プログラムとを、実装したコン 及UMMTプラウザとの間でデータの送受信を行うデータ された範囲のみを復号するデータ復号手段と8787サーバ [0117] 同様に、特に、データ復号装置を、RMTプ

やプラウザに影響を与えることがない。 用して暗号処理命令を定義するため、既存のMMサーバ 【0 1 1 8】また、特に、HTML台語のコメント命令を利

# 【図酒の餌単な説明】

4の全体構成図 【図1】本発明の実施の形態1のデータ暗号通信システ

**ータ暗号通信システムの全体構成図** 【図3】暗号化プロキシ及び復号プロキシを利用したデ 【図2】データ送信装置及びデータ受信装置の構成図

【図4】データ暗号化手段及びデータ復号手段の詳細構

【図5】 暗号化対象データ及び暗号化データのデータ模

【図6】昭号処理命令の一覧を示す図

【図7】全体の動作概略を示すフローチャート

【図8】ユーザ鍵生成処理のフローチャート

【図9】 データ作成処理のフローチャート

【図11】データ暗号化手段及びデータ復号手段の処理 【図10】データ取得処理のフローチャート

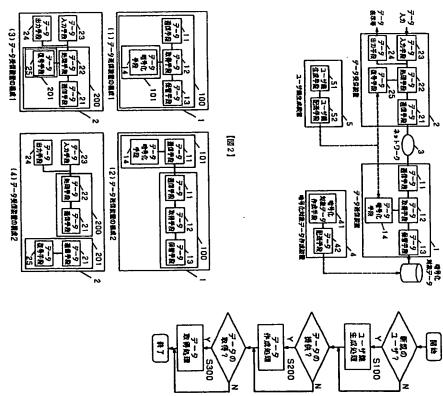
のフローチャート

- タ取得処理のフローチャート 【図12】 晴号化プロキシ及び復号プロキシ利用時のテ

> テムの全体構成図 ーチャーァ 【図13】本発明の実施の形態2のデータ暗号通信シス 【図16】復号プロキシ利用時のデータ取得処理のフロ 【図15】データ取得処理のフローチャート 【符号の説風】 【図14】データ作成処理のフローチャート 200 MMアラウザ 101 時号プロキシ 25 データ復号手段 14 データ暗号化手段 5 ユーザ鍵生成物質 データ受信装置 暗号化対象データ作成校団

Ⅰ データ送信装置 201 彼号プロキシ

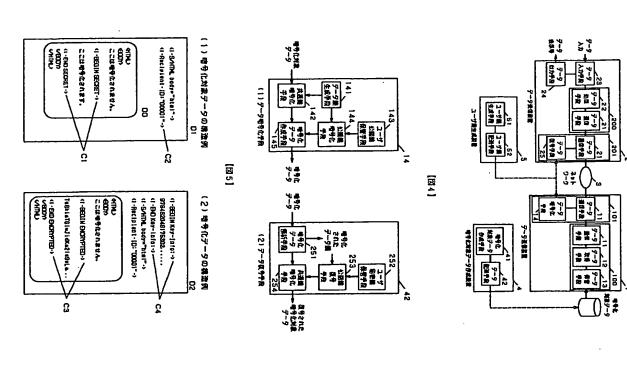
[図7]

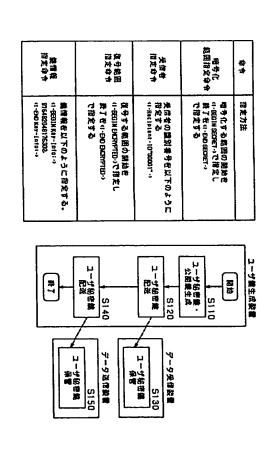


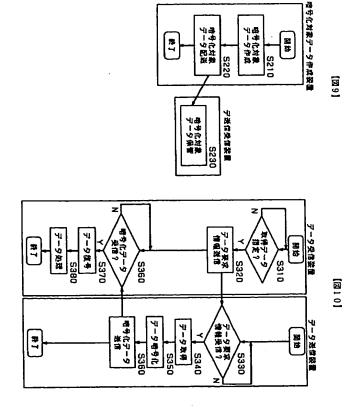
[図3]

[日日]

[8四8]







- 15 -

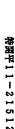
データ電号化処理 (5350)

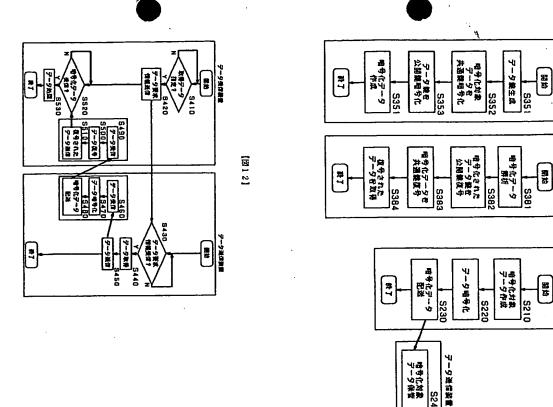
データ暗号手段

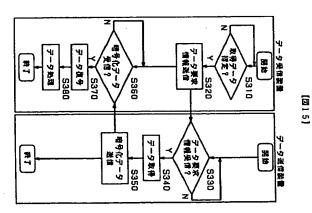
暗号化データ作成装置

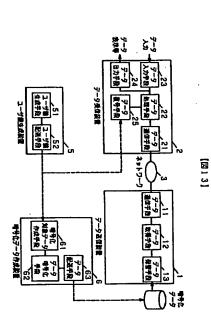
[図14]

[[2] 1 1]









- 18 -

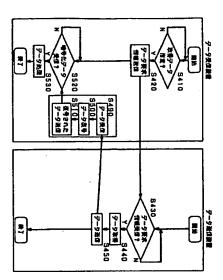
- 17 -

フロントページの投き

(72)発明者 西族 丘 受知県名古昭市中区衆2丁目6番1号白川 ビル別館5階 株式会社松下電器情報シス

テム名古恩研究所内

(72)発明者 小野 黄敏 愛知県名古壁市中区衆2丁目6番1号白川 ビル別館5階 株式会社松下電器情報システム名古屋研究所内



[四16]

- 19 -